PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-257047
(43)Date of publication of application : 25.09.1998

(51)Int.Cl. H04L 9/32
G09C 1/00
H04L 9/08

(21)Application number : 09-057515
(22)Date of filing : 12.03.1997

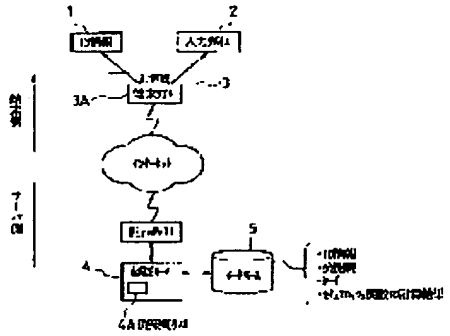
(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : KAWABE KAZUHIRO

(54) AUTHENTICATION SYSTEM AND PUBLIC KEY MANAGEMENT SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To authenticate an individual on-line and to make only the individual able to abandon and update a public key by executing a unidirectional function to a terminal software prior to the start of communication and transmitting a calculated result to a host side by a terminal side and collating the calculated result with a true value and detecting whether or not the terminal software is altered by a server side.

SOLUTION: A terminal software 3A substitutes a terminal software 3A to a secure hash function and transfers the calculated result to an authentication server 4. An authentication server 4 compares the received calculated result with a stored value, and when they match, judges that the alteration of a third person does not reach the terminal software 3A and shifts to the processing of authenticating whether or not a person requesting the abandonment of the public key is a true owner. The true owner is authenticated by transmitting a 'seed' to the terminal software 3A. Thus, even in the case that a secret key is stolen, only the individual is surely authenticated and the public key is safely and quickly abandoned.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－257047

(43)公開日　平成10年(1998)９月25日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｚ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｅ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｆ
					６７５Ｄ

審査請求　未請求　請求項の数５　ＯＬ　（全 11 頁）

(21)出願番号　特願平９－57515

(22)出願日　平成９年(1997)３月12日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　河辺　和宏
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

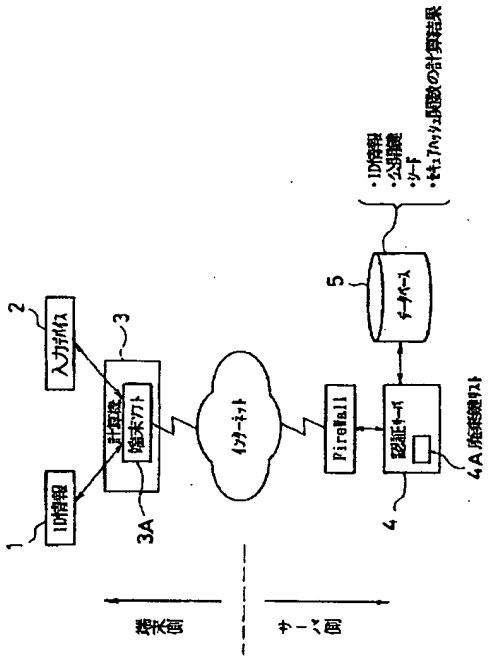
(74)代理人　弁理士　工藤　宣幸

(54)【発明の名称】　不正検出システム及び公開鍵管理システム

(57)【要約】

【課題】　オンラインによる公開鍵の安全な破棄／更新を可能とする。

【解決手段】　操作用の端末側に、通信の開始に先立って、端末上で動作する端末ソフトに一方向性関数を施し、その算出結果をホスト側へ送信する算出結果送信手段を設ける。一方、当該端末とネットワークを介して接続されたサーバ側に、ネットワークを介して受信された算出結果と、予め格納されている当該算出結果に対応する真の値とを照合し、端末ソフトに改変が加えられていないか検出する不正有無検出手段とを設ける。これにより、利用者が知らない間に、盗聴者等によって端末ソフトの一部が不正に改変されても、その改変を使用前に確認できるようにする。



1

【特許請求の範囲】

【請求項１】　操作用の端末と、当該端末に対してネットワークを介して接続されたサーバとによって構成される不正検出システムにおいて、

端末側に設けられ、通信の開始に先立って、端末上で動作する端末ソフトに一方向性関数を施し、その算出結果をホスト側へ送信する算出結果送信手段と、

サーバ側に設けられ、ネットワークを介して受信された上記算出結果と、予め格納されている当該算出結果に対応する真の値とを照合し、上記端末ソフトに改変が加えられていないか検出する不正有無検出手段とを備えることを特徴とする不正検出システム。

【請求項２】　操作用の端末と、当該端末に対してネットワークを介して接続されたサーバとによって構成される不正検出システムにおいて、

端末側に設けられ、通信の開始に先立って、入力デバイスのドライバソフトに一方向性関数を施し、その算出結果をホスト側へ送信する算出結果送信手段と、

サーバ側に設けられ、ネットワークを介して受信された上記算出結果と、予め格納されている当該算出結果に対応する真の値とを照合し、上記ドライバソフトに改変が加えられていないか検出する不正有無検出手段とを備えることを特徴とする不正検出システム。

【請求項３】　公開鍵を保管するサーバと、当該サーバに対してネットワークを介して接続された端末とによって構成される公開鍵管理システムにおいて、

上記サーバは、一の公開鍵について用意された複数個のサブコードそれぞれについて与えられる真の認証用コードに一方向性関数を施すことにより得られる値と、各サブコードとの組を複数個記憶する記憶手段と、認証時、上記記憶手段から任意に選択した一のサブコードを上記端末へ送信するサブコード送信手段と、上記サブコードに対して上記端末から応答のあった値と上記記憶手段に予め記憶している当該サブコードに対する真の値とを照合し、上記端末の操作者が真の利用者か否か判定する判定手段とを備えることを特徴とする公開鍵管理システム。

【請求項４】　公開鍵を保管するサーバと、当該サーバに対してネットワークを介して接続された端末とによって構成される公開鍵管理システムにおいて、

上記端末は、上記サーバから受信したサブコードと操作者が入力した任意の入力コードから認証用コードを生成する認証用コード生成手段と、当該認証用コードに一方向性関数を施すことにより得られる値を、上記サーバに対する応答として送信する算出結果送信手段とを備えることを特徴とする公開鍵管理システム。

【請求項５】　上記サーバは、上記判定手段により真の利用者であると判定された利用者より公開鍵の更新を指示された場合、上記記憶手段に記憶されている公開鍵についての信頼度を低い値に書き換える書換手段を備えることを特徴とする請求項３に記載の公開鍵管理システム。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば、公開鍵暗号方式を採用するネットワークシステムに適用して好適な不正検出システム及び公開鍵暗号システムに関する。

【０００２】

【従来の技術】今日における通信網の発達は目覚ましく、電子決済など新たな通信サービスの実用化が進められている。しかし、このような新たな通信サービスの実現には、ネットワーク上での存在を否定し得ない盗聴者から、通信内容を確実に保護し安全性を高める技術が不可欠となる。このため、暗号化技術を応用した各種の方法が提案されている。

【０００３】その一つが、公開鍵暗号システムである。この公開鍵暗号システムは、送信側の暗号化と受信側の復号とで異なる二つの鍵を用いるもので、秘密鍵を有するものだけが公開鍵で暗号化された通信文を復号できるというものである。さて、かかるシステムでは、公開鍵が真に取引相手の所有物であることが保証されていることが前提となる。なぜなら、他人が真の取引相手になりすまして公開した公開鍵であれば、真の取引相手になりすました他人を取引相手とすることになるからである。

【０００４】そこで、本システムでは、他者に侵害されない認証サーバ上に公開鍵を登録する方式を採用している。認証サーバに公開鍵を登録するためには本人であることを証明する物証が必要であり、通常、オフラインで所定の手続が行われる。同様に公開鍵の抹消も本人であることを証明する必要があるため、通常、オフラインで行われている。

【０００５】

【発明が解決しようとする課題】しかし、オフラインでの公開鍵の登録／抹消は、多くの場合、ある程度の日数を要するため、秘密鍵が盗難又は紛失等に遭遇した場合にも被害を最小限に抑えることができない。すなわち、秘密鍵を取得した他者は、公開鍵が抹消されるまで秘密鍵の所有者になりすますことが可能であり、真の所有者が盗聴者による不正な商取引などで被害を被るおそれがある。

【０００６】このため、このような場合には、早急に鍵を抹消できることが望まれている。現在、かかる公開鍵を管理する認証サーバに対する公開鍵の抹消プロトコルとしては“ＩＴＵ－Ｔ Recommendation X.509”が存在するが、このプロトコルには、本人認証についての規定がないのが現状である。

【０００７】しかし、鍵の抹消を本人の認証なく行えることとすると、本人以外の者が勝手に鍵の抹消を行うことができてしまう。

【０００８】本発明は以上の点を考慮してなされたもの

で、オンライン上での本人の認証を可能とし、本人のみが公開鍵の破棄／更新を行える安全性の高い公開鍵管理システムを提案しようとするものである。また、これに関連して、オンライン手続の安全性を高める不正検出システムを提案しようとするものである。

【０００９】

【課題を解決するための手段】

（Ａ）かかる課題を解決するため第１の発明においては、操作用の端末と、当該端末に対してネットワークを介して接続されたサーバとによって構成される不正検出システムにおいて、以下の手段を備えるようにする。

【００１０】すなわち、(1) 端末側に設けられ、通信の開始に先立って、端末上で動作する端末ソフトに一方向性関数を施し、その算出結果をホスト側へ送信する算出結果送信手段と、(2) サーバ側に設けられ、ネットワークを介して受信された算出結果と、予め格納されている当該算出結果に対応する真の値とを照合し、端末ソフトに改変が加えられていないか検出する不正有無検出手段とを備えるようにする。

【００１１】以上のように、第１の発明においては、利用者が知らない間に、盗聴者等によって端末ソフトの一部が不正に改変されているようなことがあっても、その改変が一方向性関数を施した値の不一致として、不正有無検出手段で検出されることになる。

【００１２】（Ｂ）また、第２の発明においては、操作用の端末と、当該端末に対してネットワークを介して接続されたサーバとによって構成される不正検出システムにおいて、以下の手段を備えるようにする。

【００１３】すなわち、(1) 端末側に設けられ、通信の開始に先立って、入力デバイスのドライバソフトに一方向性関数を施し、その算出結果をホスト側へ送信する算出結果送信手段と、(2) サーバ側に設けられ、ネットワークを介して受信された算出結果と、予め格納されている当該算出結果に対応する真の値とを照合し、ドライバソフトに改変が加えられていないか検出する不正有無検出手段とを備えるようにする。

【００１４】以上のように、第２の発明においては、利用者が知らない間に、盗聴者等によって入力デバイスのドライバソフトの一部が不正に改変されているようなことがあっても、その改変が一方向性関数を施した値の不一致として、不正有無検出手段で検出されることになる。

【００１５】（Ｃ）さらに、第３の発明においては、公開鍵を保管するサーバと、当該サーバに対してネットワークを介して接続された端末とによって構成される公開鍵管理システムにおいて、以下の手段を備えるようにする。

【００１６】すなわち、サーバは、(1) 一の公開鍵について用意された複数個のサブコードそれぞれについて与えられる真の認証用コードに一方向性関数を施すことにより得られる値と、各サブコードとの組を複数個記憶する記憶手段と、(2) 認証時、記憶手段から任意に選択した一のサブコードを端末へ送信するサブコード送信手段と、(3) サブコードに対して端末から応答のあった値と記憶手段に予め記憶している当該サブコードに対する真の値とを照合し、端末の操作者が真の利用者か否か判定する判定手段とを備えるようにする。

【００１７】以上のように、第３の発明においては、認証時に用いられるサブコードとしていつも異なる値を使用することとし、ネットワークを介して応答される値もその都度異なる値となるようにしたことにより、ネットワークを介しての認証の安全性を高めることが可能となる。

【００１８】（Ｄ）さらに、第４の発明においては、公開鍵を保管するサーバと、当該サーバに対してネットワークを介して接続された端末とによって構成される公開鍵管理システムにおいて、以下の手段を備えるようにする。

【００１９】すなわち、端末は、(1) サーバから受信したサブコードと操作者が入力した任意の入力コードから認証用コードを生成する認証用コード生成手段と、(2) 当該認証用コードに一方向性関数を施すことにより得られる値を、サーバに対する応答として送信する算出結果送信手段とを備えるようにする。

【００２０】以上のように、第４の発明においては、認証を行うサーバから与えられたサブコードに操作者が入力した任意の入力コードから生成した認証用コードに一方向性関数を施して得られた値を送信することとしたことにより、操作者本人のみが知り得る入力コードの秘匿性を一段と高めることが可能となる。

【００２１】

【発明の実施の形態】

（Ａ）第１の実施形態

以下、本発明に係る不正検出システム及び公開鍵管理システムの第１の実施形態を、図面を用いて説明する。

【００２２】（Ａ－１）第１の実施形態の構成

図１は、第１の実施形態に係るシステムの機能ブロック図である。図１に示すように、本システムは、インターネット等の通信網を介して接続された端末側装置とサーバ側装置とで構成される。ここで、端末側装置は、本システムを利用する商店や個人宅（家庭）等に存在する装置である。すなわち、ユーザが最寄りの入力端末から早急に公開鍵の破棄を行うことができることを前提としている。

【００２３】まず、端末側装置の構成を説明する。この実施形態における端末側装置は、入力デバイス２と、計算機３と、端末ソフト３Ａとによって構成され、ＩＤ情報１が使用時に入力されるようになっている。

【００２４】このＩＤ情報１は、鍵保有者のＩＤであり、英数字又は数字のみで表現された値である。ＩＤ情

報１は、ユーザが入力する場合とＩＣカードなどのデバイスから入力される場合がある。勿論、ＩＣカードが盗難にあった場合は、予め記録しておいたＩＤ情報１をユーザが入力する必要がある。これに対し、不正利用を本人が気づいた場合には、手元に存在するＩＣカード等からＩＤ情報１に対応する所定の値が入力される。

【００２５】入力デバイス２は、キーボード（テンキーのみの場合も含む）、圧感タブレット、マイクなどのデバイスである。入力デバイス２は、セキュリティとコストの関係で選択する必要がある。圧感タブレットやマイクによる情報を用いれば、精度の高い個人認証を行うことができるが、ただ単にキー入力のみでは個人認証の精度は低い。しかし、キー入力のみでもタイピングパターン（タイピング速度による認証）を用いることにより個人認証の精度をあげることは可能である。

【００２６】なお、この認証システムでは、秘密鍵が平文（暗号文でないテキスト）で格納されているシステムではなく、秘密鍵も暗号化した結果を保存していることを想定している。そのため、入力デバイス２から入力されたデータをセキュアハッシュ関数にかけた結果が秘密鍵の暗号化鍵として働くか否かによって本人認証を行う。すなわち、秘密鍵を利用した秘密通信においても使用するデバイスであり、入力デバイス２は公開鍵の破棄のために必要な特別なデバイスではない。なお、セキュアハッシュ関数は、実際上計算量の点で逆関数の計算が困難な関数、すなわち、一方向性関数の一つである。

【００２７】端末ソフト３Ａは、ユーザインターフェースの制御、認証サーバとの通信、暗号化処理（すなわち、認証サーバ４の公開鍵を用いた認証サーバ４の認証処理）を行うための手段である。また、この端末ソフト３Ａが保持されているマシンのセキュリティ度によって、初期処理の動作が異なる。

【００２８】一方、サーバ側装置は、認証サーバ４と、廃棄鍵リスト４Ａと、データベース５とによって構成されている。

【００２９】ここで、認証サーバ４は、データベース５の情報を基に、内容が正しいという認証を付加するために存在する手段であり、実際上は、計算機で動作するソフトウェア処理により実現されている。ここで、認証サーバ４は、端末ソフト３Ａに対する自己の認証を認証サーバ４の秘密鍵を用いて行うようになっている。従って、認証サーバ４の秘密鍵は厳重に管理する必要がある。なお、この秘密鍵が漏洩した場合には、認証サーバ４の存在が危険となるので、早急な対処が必要となる。このため、認証サーバ４やデータベース５は、ファイアウォールなどにより第三者から守られている。

【００３０】廃棄鍵リスト４Ａは、認証サーバ４のキャッシュメモリ上に記憶されているリストである。これらは、認証サーバ４での認証により本人であると確認された者、又は、オフラインにより本人であると確認された

者から申請のあった公開鍵の廃棄を記憶するのに用いられる。

【００３１】データベース５は、「ＩＤ情報」、「公開鍵」、「シード（認証用のデータ）」、「セキュアハッシュ関数の結果」を項目とするデータである。なお、シード、セキュアハッシュ関数の結果の項は、１つのＩＤ情報に対して複数存在している。因みに、このデータベース５に保存している内容が第三者に漏洩することは望ましくないが、仮に漏洩しても、改変されなければ致命的ではない。これは、なんらかの方法により外部に洩れても、第三者の悪用が困難なデータのみが格納されていることによる。

【００３２】（Ａ－２）第１の実施形態の動作

以上の構成において、実施形態に係る公開鍵管理システムを用いた公開鍵の破棄申請動作を説明する。

【００３３】（Ａ－２－１）不正検出動作の必要性

この破棄申請動作は、秘密鍵を盗難等されたユーザによる入力端末を用いた破棄申請から開始される。

【００３４】しかしながら、その初期動作は、入力端末としてどのような装置を使用できるかによって異なることになる。例えば、理想的な入力端末、すなわち、専用端末であって、ユーザが入力に使用するプログラムを改変できないものであり（例えば、プログラムがＲＯＭに書き込まれていて書き換えが不可能であり）、かつ、端末操作中は外部から操作内容への接続を遮断できる端末の場合には、後述する不正検出動作は不要となる。

【００３５】しかし、一般に、個人が家庭で用いる計算機３は、端末ソフト３Ａを書き換え可能なメモリ（ＲＡＭ）に保存する構成になっているので、端末ソフト３Ａが改変されている可能性がある。また、端末ソフト３Ａが改変されるおそれがないとしても、端末操作中における入力デバイス２への操作が外部から監視し得る端末の場合には、操作が盗聴される可能性がある。

【００３６】そこで、以下の説明では、かかる不正な端末ソフト３Ａの改変や操作の盗聴等から公開鍵の破棄申請動作を未然に防止する不正検出動作を含む公開鍵破棄申請動作を説明する。

【００３７】（Ａ－２－２）不正検出動作を含む公開鍵破棄申請動作例

（ａ）呼の設定

図２は、このように侵害されている可能性がある又は盗聴の可能性のある信頼性の低い計算機３を入力端末として使用する場合の破棄申請処理を表した図である。なお、図２の処理（１）に達するまでの処理は、呼設定のための継続処理であるので、ここでは説明を省略する。因みに、この処理の過程において、端末ソフト３Ａは、これから通信する相手が認証サーバ４であることを、認証サーバ４の公開鍵を用いた暗号処理によって認証する。

【００３８】（ｂ）処理（１）

7

処理（１）は、端末ソフト３Ａが改変されていないことを確かめるための不正検出処理である。ここで、端末ソフト３Ａは、セキュアハッシュ関数ＭＤを使用する。セキュアハッシュ関数ＭＤは、入力するデータが異なると出力値が異なる関数であり、短いデータにより改変されているか否かを判断できるものである。この処理（１）の段階で、端末ソフト３Ａは、セキュアハッシュ関数ＭＤに当該端末ソフト３Ａを代入して計算し、計算結果ＭＤｔを求める。また、同じく、端末ソフト３Ａは、セキュアハッシュ関数ＭＤに入力デバイス２をドライブするドライバソフトとネットワーク（通信用）ドライバソフトを代入して計算し、計算結果ＭＤｄを求める。

【００３９】（ｃ）処理（２）

次の処理（２）では、先に求めた計算結果ＭＤｔ、ＭＤｄと、ユーザ識別子のＩＤを認証サーバ４に署名付きで転送する。なおこのとき、端末ソフト３Ａは、認証サーバ４に対して端末タイプを示すＩＤｍも転送する。

【００４０】（ｄ）処理（３）

処理（３）からは、認証サーバ４での処理に移る。認証サーバ４は、端末ソフト３Ａからこれら情報（すなわち、ＭＤｔ、ＭＤｄ、ＩＤｍ、ＩＤ）を受信すると、端末タイプを表す情報ＩＤｍから該当する端末ソフト３Ａをセキュアハッシュ関数で計算した場合に得られるものとして記憶されている計算結果と、実際に転送されてきた計算結果ＭＤｔとを比較し、両者が一致するか否か判定する。

【００４１】ここで、認証サーバ４は、両者が一致しているとき、端末ソフト３Ａに第３者の改変が及んでないと判定し、両者が一致していないとき、端末ソフト３Ａに第３者の改変が及んでいると判定する。同様に、デバイスドライバについても、改変の有無を判定する。

【００４２】以上の処理が前述した不正検出動作である。ここで、端末ソフト３Ａ及びデバイスドライバの双方共に改変が及んでいないことが確認されると、以下説明する公開鍵の破棄を申請している者が真の所有者であるか否かを認証する処理に移行する。なお、いずれか一方でも一致しないことが確認された場合には、認証サーバ４より端末ソフト３Ａに対してメッセージが送信される。

【００４３】（ｅ）処理（４）

処理（４）から認証処理に移行する。この認証処理に移行すると、認証サーバ４は、端末ソフト３Ａから受信したユーザ識別子ＩＤを用いてデータベースを検索し、当該ＩＤに対して登録されている、「シード」と「セキュアハッシュ関数の計算結果の組み合わせの集合の中から任意に一つを選択する。そして、認証サーバ４は、このうち「シード」のみを、署名付きで端末ソフト３Ａ側に送信する。この認証サーバ４から端末ソフト３Ａへの「シード」の送信動作は、認証サーバ４から端末ソフト３Ａへの「誰何」（Challenge）に当たる。

8

【００４４】なお、この「シード」は、本人のみが入力できる情報を隠蔽しつつ、本人であることを認証する上で重要な役割を果たすデータであり、秘密保持のため、一度使用した「シード」は二度と使用しない。従って、「シード」を補充する必要が生じた場合には、セキュリティが十分保たれたシステム（オフライン又は安全の確かめられている専用端末）で作成し、データベース５に登録する。因みに、「シード」は英字や数字等で与えられる。

【００４５】（ｆ）処理（５）

処理（５）からは、再び、端末ソフト３Ａ側の処理に移行する。まず、端末ソフト３Ａは、認証サーバ４から「シード」及び「証明書」を受け取ることにより、自らにソフトウエア上の改変がないことを確認し、当該検出動作のプログラムを終了する。そして、以後、自分こそ本人であることを認証サーバ４に認証させるための動作に移行する。ただし、この段階においても、端末ソフト３Ａを動かしている計算機３に第三者が存在していたり、又は、第三者が不正に動作させている隠しプログラムが存在する危険性があるので、端末ソフト３Ａは、関係するデバイス（セキュアハッシュ関数でチェックしたデバイス）をロックし、第三者が端末ソフト３Ａに対して行う操作を覗くことができないようにする。

【００４６】（ｇ）処理（６）

処理（６）では、ユーザにより、入力デバイス２を用いて、本人のみが知り得る「データ列」が与えられる。ここで入力される「データ列」は、個人を認証するためのデータであり、例えば、パスワードが該当する。

【００４７】（ｈ）処理（７）

処理（７）では、入力デバイス２から入力された「データ列」と認証サーバ４から与えられた「シード」とから新たな英数字列が作成される。例えば、「データ列」を「ｄｆ」とし、「シード」を「ａｂｃ」とするとき、新たな英数字列として「ａｂｃｄｆ」が作成される。なお、入力された「データ列」は、計算機３のメモリとレジスタから共に削除され、漏洩を防ぐ処理が行われる。

【００４８】このように新たな英数字列が作成されると、端末ソフト３Ａは、これをセキュアハッシュ関数に代入して計算し、その結果ＭＤｐを生成する。この結果ＭＤｐは、本人のみしか知り得ない「データ列」と「シード」から一意に定まる値である。なお、以上から分かるように、この認証動作では、秘密鍵を一切必要としない。従って、第３者は、秘密鍵を取得し得たとしても、ここで入力される「データ列」が分からない限り、本人に成り代わることはできない。

【００４９】（ｉ）処理（８）

処理（８）では、端末ソフト３Ａから新たに作成された英数字列について算出された計算結果ＭＤｐが認証サーバ４に署名付きで送信される。この送信動作は、認証サーバ４から端末ソフト３Ａになされた「誰何」（Challe

nge ）に対する「応答」（Response ）に当たる。

【００５０】（ｊ）処理（９）

処理（９）は、認証サーバ４側の処理である。認証サーバ４は、端末ソフト３Ａから応答のあった計算結果ＭＤｐと、先に使用した「シード」と組として格納されている「セキュアハッシュ関数の結果」とを比較する。ここで、両結果が同一であれば、通信相手が本人であることが確認される。

【００５１】このように本人であることが認証された段階で、認証サーバ４は、今回の破棄申請の対象となった共通鍵を廃棄鍵リスト（Certificate Revocation List：CRL）４Ａに加える。そして、破棄申請が受理されたことを、ユーザ（端末ソフト３Ａ）にメッセージとして送る。なお、更新鍵リスト（Certificate Renovation List：CRL）４Ｂを作成するか否かと、データベース５の更新については認証サーバ４の仕様であり、ここでは言及しない。

【００５２】（ｋ）処理（１０）

処理（１０）では、端末ソフト３Ａが、認証サーバ４から破棄申請の受理確認を受け、一連の処理を終了して呼の解放がなされる。

【００５３】（Ａ－３）第１の実施形態の効果

以上のように、第１の実施形態によれば、公開鍵の破棄申請に先だって、破棄申請に使用される端末ソフト３Ａや入力デバイス２が改変されているおそれがないかを検査する不正検査処理を行うようにしたことにより、安全な専用端末を利用する場合と近い端末になり得る。

【００５４】また、実際に、公開鍵の破棄申請の際には、本人のみが入力できる「データ列」の入力をすでに安全性が確かめられたデバイスのみがロックされた状態で入力できるようにし、かつ、その際入力された「データ列」はメモリ等からすぐさま破棄するようにしたので、かかる入力段階での盗難のおそれも回避できる。

【００５５】さらに、オンラインでの公開鍵の破棄申請を受け付ける認証サーバ４に、「シード」とそれに対する本人のみが知り得る計算結果を組として記憶させておき、破棄申請時には、認証サーバ４から破棄申請を出している端末ソフト３Ａに任意の選択した「シード」を送って、これに対する端末ソフト３Ａからの応答が当該「シード」について組として保持されている値と一致するか否かに基づいて本人か否かを認証するようにしたことにより、秘密鍵を盗難された場合であっても確実に本人のみを認証でき、安全かつ早急に公開鍵の破棄を実現できる。

【００５６】なお、この公開鍵の破棄申請では、秘密鍵を利用した秘密通信で使用するデバイスのみを利用するために安価にシステムを構築できる。

【００５７】また、認証サーバ４が参照するデータベース５には、本人のみが知りうる情報が記録されていないため、仮に漏洩してもデータの改竄が行われない限り、

破棄申請を安全に実行することができる。

【００５８】（Ｂ）第２の実施形態

以下、本発明に係る不正検出システム及び公開鍵管理システムの第２の実施形態を、図面を用いて説明する。

【００５９】一般に、秘密鍵の漏洩に気づいた後も、早急にＩＣカード等を使用しなければならない状況は発生し得る。このような場合、従来は、秘密鍵が漏洩したまま危険と知りつつ使用するか、盗聴に対して安全な端末が存在するサービスセンター等で公開鍵（すなわち、秘密鍵）の更新を行う必要がある。しかし、前者の場合には、不正利用か否かを判断できないという欠点がある。また、後者の場合には、更新できる時間帯がサービスセンター等を使用できる時間帯に制限される他、サービスセンター等が更新を希望するユーザの近くに存在しなければならないという制約があった。

【００６０】そこで、この第２の実施形態では、オンライン上で公開鍵を更新する方法について説明するものである。

【００６１】（Ｂ－１）第２の実施形態の構成

図３は、第２の実施形態に係るシステムの機能ブロック図である。図３は、図１との同一、対応部分に同一、対応符号を付して示すものである。

【００６２】図３と図１との違いは、端末側にＩＣカード等に記憶されている秘密鍵を更新する秘密鍵更新デバイス３Ｂを設ける点と、認証サーバ４のキャッシュメモリ上に廃棄鍵リスト４Ａに代えて更新鍵リスト４Ｂを記憶させる点、及び、データベース５上に「セキュアハッシュ関数の結果に対するセキュリティレベル」を追加記憶させる点の３つである。

【００６３】（Ｂ－２）第２の実施形態の動作

以下、第２の実施形態に係る公開鍵管理システムを用いた公開鍵の更新申請動作を説明する。なお、図４は、侵害の可能性がある又は盗聴の可能性のある信頼性の低い計算機３を入力端末として使用する場合の更新申請処理を表した図である。このうち、処理（１）～処理（８）までの処理内容は、第１の実施形態と同様であるため、ここでは、処理（９）以降の処理について説明する。

【００６４】（ａ）処理（９）

処理（９）は、認証サーバ４側の処理である。認証サーバ４は、端末ソフト３Ａから応答のあった計算結果ＭＤｐと、先に使用した「シード」と組として格納されている「セキュアハッシュ関数の結果」とを比較する。ここで、両結果が同一であれば、通信相手が本人であることが確認される。このように本人であることが認証されると、認証サーバ４は、認証できたことをユーザ（端末ソフト３Ａ）にメッセージとして送る。

【００６５】（ｂ）処理（１０）

処理（１０）は、端末ソフト３Ａ側の処理である。この段階で、端末ソフト３Ａは、認証された本人からの指示に基づいて、新たな公開鍵（ＰＫ）と秘密鍵（ＳＫ）を

11

生成する。なお、新たに作成された秘密鍵（ＳＫ）は、秘密鍵更新デバイス３Ｂにより、ＩＣカード等の安全なデバイスに格納される。

【００６６】（ｃ）処理（１１）

処理（１１）では、生成された公開鍵（ＰＫ）が認証サーバ４に送信される。

【００６７】（ｄ）処理（１２）

処理（１２）は、認証サーバ４側の処理である。ここで、認証サーバ４は、受信された公開鍵（ＰＫ）を、更新鍵リスト（Certificate Renovation List：ＣＲＬ）に加える。また、認証サーバ４は、更新申請が受理されたことを、メッセージとしてユーザ（端末ソフト３Ａ）に通知すると共に、データベース５のセキュリティレベルを下げる処理を行う。

【００６８】ここで、セキュリティレベルは公開鍵（ＰＫ）の信頼度であり、オンラインでは通信の途中で悪意の第三者がコネクションが確立してからハイジャックして、正規ユーザになりすます可能性があることを表現している。クレジットカードではこの信頼度を利用限度額にマッピングすることにより、リスクの少ない運営が可能となる。また、このセキュリティレベルを上げるにはセキュリティが保たれたシステムで再確認する必要がある。

【００６９】（ｅ）処理（１３）

処理（１３）は、認証サーバ４から更新申請の受理確認を受けた端末ソフト３Ａが、一連の処理を終了して呼の解放を行う処理である。

【００７０】（Ｂ－３）第２の実施形態の効果

以上のように、第２の実施形態によれば、公開鍵の更新申請に先だって、更新申請に使用される端末ソフト３Ａや入力デバイス２が改変されているおそれがないかを検査する不正検査処理を行うようにしたことにより、安全な専用端末を利用する場合と近い端末になり得る。

【００７１】また、実際に、公開鍵の更新申請の際には、本人のみが入力できる「データ列」の入力をすでに安全性が確かめられたデバイスのみがロックされた状態で入力できるようにし、かつ、その際入力された「データ列」はメモリ等からすぐさま破棄するようにしたので、かかる入力段階での盗難のおそれも回避できる。

【００７２】さらに、オンラインでの公開鍵の更新申請を受け付ける認証サーバ４に、「シード」とそれに対する本人のみが知り得る計算結果を組として記憶させておき、更新申請時には、認証サーバ４から更新申請を出している端末ソフト３Ａに任意の選択した「シード」を送って、これに対する端末ソフト３Ａからの応答が当該「シード」について組として保持されている値と一致するか否かに基づいて本人か否かを認証するようにしたことにより、秘密鍵を盗難された場合であっても確実に本人のみを認証でき、安全かつ早急に公開鍵の更新を実現できる。

12

【００７３】さらに、公開鍵の更新がオンラインで行われた場合には、セキュリティー情報としてデータベース５に記憶するようにし、その際、信頼性の高さを示すセキュリティー情報を低下させるようにしたことにより、より安全に取引等を行うことを可能とする公開鍵管理システムを実現することができる。

【００７４】（Ｃ）他の実施形態

なお、上述の実施形態においては、本発明に係る不正検出システムを公開鍵システムにおける端末ソフト３Ａや入力デバイス２の改変有無の検査に用いる場合について述べたが、これに限らず、他のシステムにおいて使用しても良い。

【００７５】

【発明の効果】以上のように、第１の発明によれば、操作用の端末側に、通信の開始に先立って、端末上で動作する端末ソフトに一方向性関数を施し、その算出結果をホスト側へ送信する算出結果送信手段を設けると共に、端末とネットワークを介して接続されたサーバ側に、ネットワークを介して受信された算出結果と、予め格納されている当該算出結果に対応する真の値とを照合し、端末ソフトに改変が加えられていないか検出する不正有無検出手段とを設けることにより、利用者が知らない間に、盗聴者等によって端末ソフトの一部が不正に改変されても、その改変を使用前に確認することができる不正検出システムを実現することができる。

【００７６】また、第２の発明によれば、操作用の端末側に、通信の開始に先立って、入力デバイスのドライブソフトに一方向性関数を施し、その算出結果をホスト側へ送信する算出結果送信手段を設けると共に、端末とネットワークを介して接続されたサーバ側に、ネットワークを介して受信された算出結果と、予め格納されている当該算出結果に対応する真の値とを照合し、ドライブソフトに改変が加えられていないか検出する不正有無検出手段とを設けることにより、利用者が知らない間に、盗聴者等によって入力デバイスのドライブソフトの一部が不正に改変されても、その改変を使用前に確認することができる不正有無検出手段を実現することができる。

【００７７】さらに、第３の発明によれば、サーバに、一の公開鍵について用意された複数個のサブコードそれぞれについて与えられる真の認証用コードに一方向性関数を施すことにより得られる値と、各サブコードとの組を複数個記憶する記憶手段と、認証時、記憶手段から任意に選択した一のサブコードを端末へ送信するサブコード送信手段と、サブコードに対して端末から応答のあった値と記憶手段に予め記憶している当該サブコードに対する真の値とを照合し、端末の操作者が真の利用者か否か判定する判定手段とを設け、認証時に用いられるサブコードとしていつも異なる値を使用できるようにしたことにより、ネットワークを介して応答される値をその都度異なる値とでき、認証時における盗聴者等のなりすま

13

しを確実に判別することができる。

【００７８】さらに、第４の発明によれば、端末に、サーバから受信したサブコードと操作者が入力した任意の入力コードから認証用コードを生成する認証用コード生成手段と、当該認証用コードに一方向性関数を施すことにより得られる値を、サーバに対する応答として送信する算出結果送信手段とを設け、認証時に応答される値がいつも異なる値になるようにしたことにより、操作者本人のみが知り得る入力コードを復号できないようにでき、認証時における盗聴者等のなりすましを確実に判別することができる。

【図面の簡単な説明】

14

【図１】第１の実施形態の構成を示すブロック図である。

【図２】図１に示すシステムで実行される不正検出処理及び公開鍵の破棄処理手順の説明に供する図である。

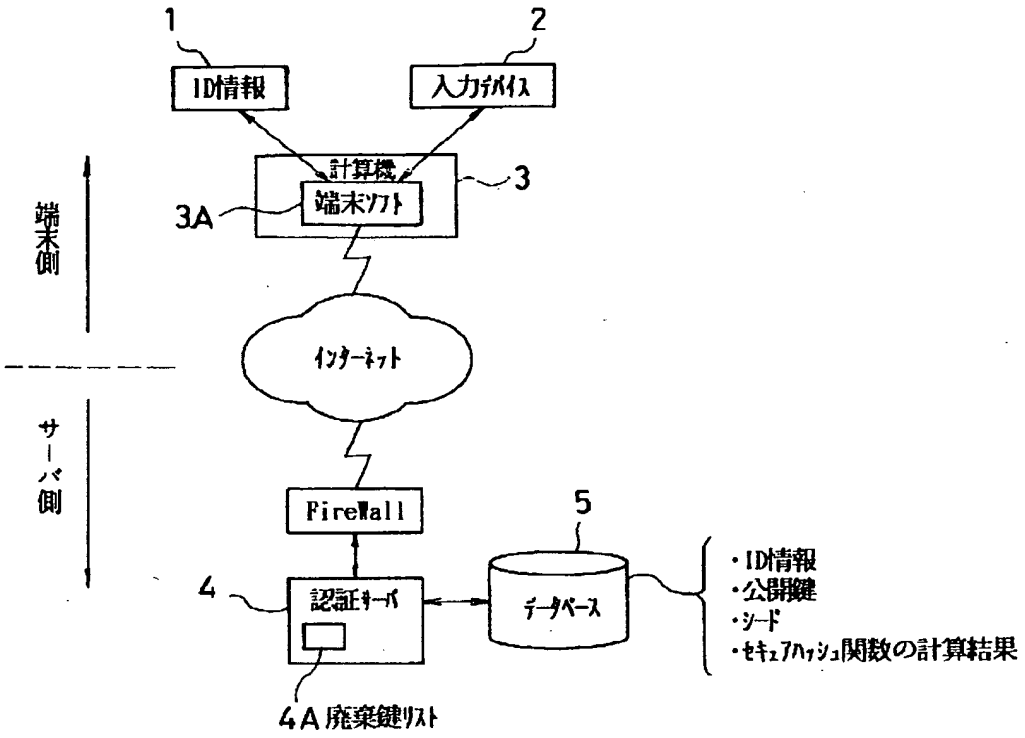
【図３】第２の実施形態の構成を示すブロック図である。

【図４】図３に示すシステムで実行される不正検出処理及び公開鍵の更新処理手順の説明に供する図である。

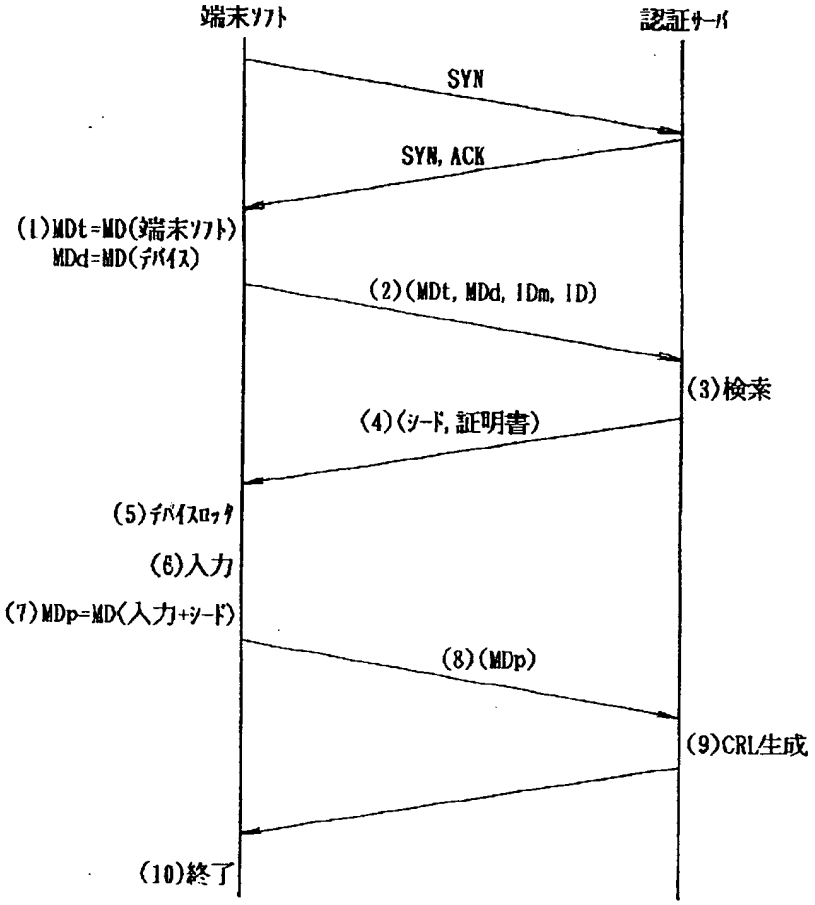
【符号の説明】

２…入力デバイス、３…計算機、３Ａ…端末ソフト、３Ｂ…秘密鍵更新デバイス、４…認証サーバ、４Ａ…廃棄鍵リスト、４Ｂ…更新鍵リスト、５…データベース。

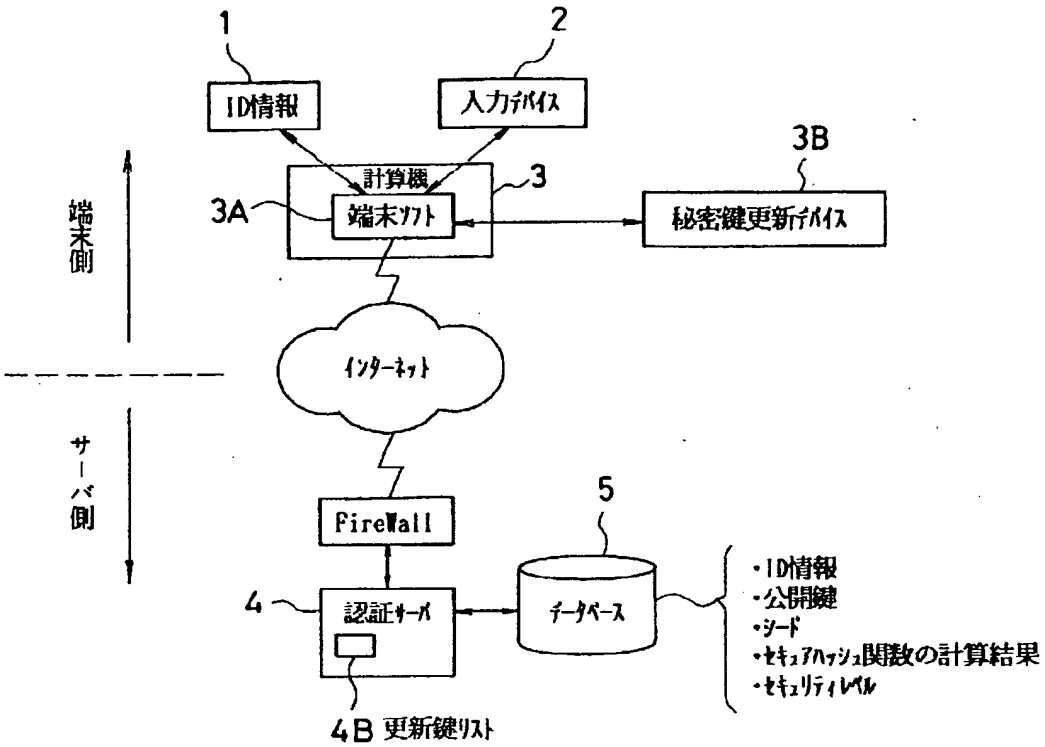
【図１】



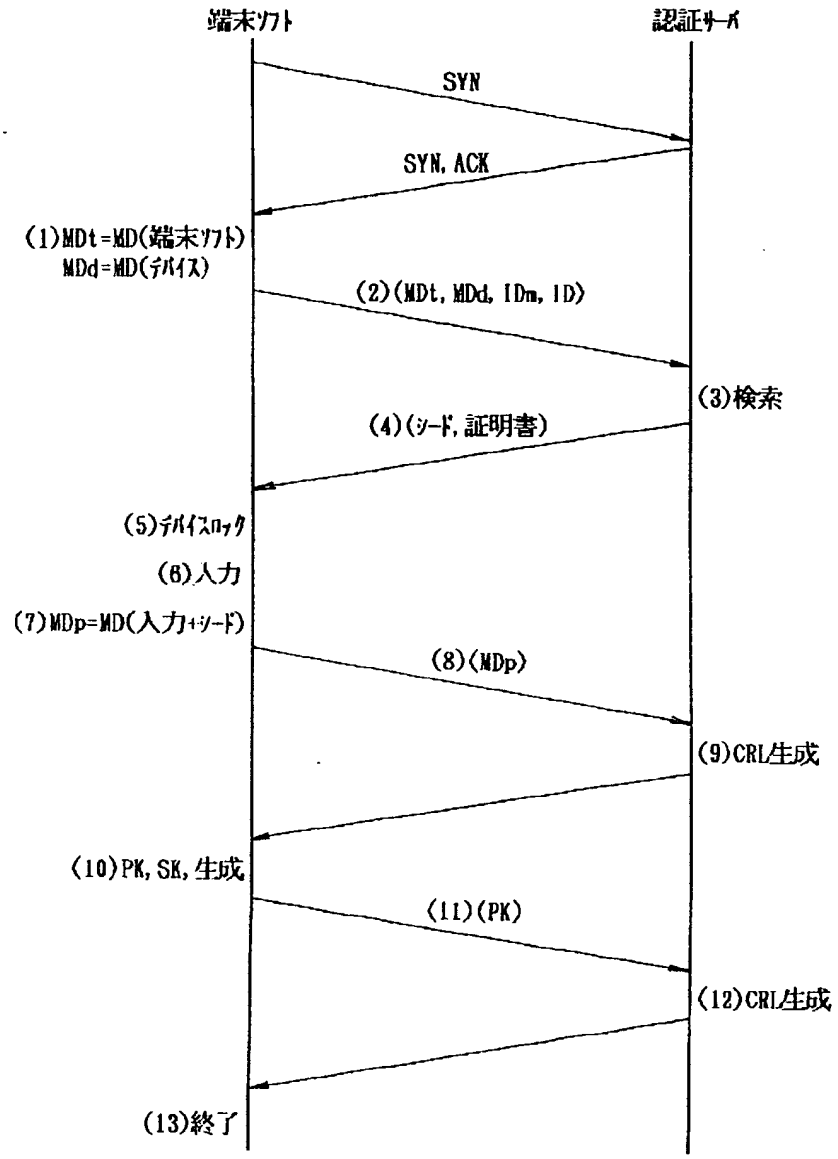
【図２】


端末ソフト
認証サーバ
SYN
SYN, ACK
(1)MDt=MD(端末ソフト)
MDd=MD(デバイス)
(2)(MDt, MDd, IDm, ID)
(3)検索
(4)(シード, 証明書)
(5)デバイスロック
(6)入力
(7)MDp=MD(入力+シード)
(8)(MDp)
(9)CRL生成
(10)終了

【図３】


1
2
ID情報
入力ﾃﾞﾊﾞｲｽ
3B
計算機
3
3A
端末ｿﾌﾄ
秘密鍵更新ﾃﾞﾊﾞｲｽ
端末側
ｲﾝﾀｰﾈｯﾄ
サーバ側
5
FireWall
4
認証ｻｰﾊﾞ
ﾃﾞｰﾀﾍﾞｰｽ
・ID情報
・公開鍵
・ｼｰﾄﾞ
・ｾｷｭｱﾊｯｼｭ関数の計算結果
・ｾｷｭﾘﾃｨﾚﾍﾞﾙ
4B 更新鍵ﾘｽﾄ

【図４】


端末ソフト
認証サーバ
SYN
SYN, ACK
(1)MDt=MD(端末ソフト)
MDd=MD(デバイス)
(2)(MDt, MDd, IDm, ID)
(3)検索
(4)(シード, 証明書)
(5)デバイスロック
(6)入力
(7)MDp=MD(入力+シード)
(8)(MDp)
(9)CRL生成
(10)PK, SK, 生成
(11)(PK)
(12)CRL生成
(13)終了